

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A network device comprising:
a processor;
a first memory, wherein
said processor and said first memory are coupled to one another;
a tunnel classification stage, wherein
said processor is coupled to control said tunnel classification stage,
said tunnel classification stage comprises
a packet processing section comprising at least one processor,
a security group identifier identification unit, coupled to said
packet processing section, and
a tunnel classification unit, coupled to said packet processing
section and said security group identifier identification unit,
said security group identifier is configured to identify a security group of a
sender of said packet,
said security group is configured to represent a plurality of senders,
said plurality of senders comprises said sender, and
said packet processing section is configured to
classify a packet based, at least in part, on a security group
identifier (SGI) of said packet, wherein
said SGI identifies said security group,
determine a routing of said packet, wherein
said packet processing section is configured to determine
said routing based, at least in part, on said SGI, and
said packet processing section is configured to determine
said routing by virtue of being configured to
identify a tunnel;
**identifying a tunnel identifier of said tunnel based on said
routing of said packet;**

determine whether forwarding said packet via said tunnel is permitted, wherein said packet processing section is configured to determine whether said forwarding is permitted based, at least in part, on said SGI, and forward said packet via said tunnel, if said forwarding said packet via said tunnel is permitted.

- 2.-3. (Cancelled)
4. (Previously Presented) The network device of claim 1, wherein said packet processing section is further configured to forward said packet through said tunnel based, at least in part, on information in a header of said packet.
5. (Cancelled)
6. (Previously Presented) The network device of claim 1, wherein a single router comprises said tunnel classification stage.
7. (Previously Presented) The network device of claim 6, wherein said tunnel classification unit comprises:
a lookup unit.
8. (Previously Presented) The network device of claim 7, wherein said lookup unit comprises:
an access control list (ACL); and
a content-addressable memory, wherein
said content-addressable memory is configured to access said ACL by
virtue of being configured to
generate an index, and
provide said index to said ACL.

9. (Previously Presented) The network device of claim 8, wherein
said network device further comprises a memory,
said ACL is stored in said memory,
said content-addressable memory and said memory are coupled to one another,
said ACL comprises a plurality of ACL entries (ACEs), and
each of said ACEs comprises a tunnel identifier field and a security group
identifier field.
10. **(Currently Amended)** A method comprising:
assigning a security group identifier (SGI) to a packet, wherein
said SGI is assigned based, at least in part, on a security group of a sender
of said packet,
said SGI identifies said security group,
said security group is configured to represent a plurality of senders, and
said plurality of senders comprises said sender;
classifying said packet based, at least in part, on said SGI;
determining a routing of said packet, wherein
said determining said routing is based, at least in part, on said SGI, and
said determining said routing comprises
identifying a tunnel;
**identifying a tunnel identifier of said tunnel based on said routing of said
packet;**
determining whether forwarding said packet via said tunnel is permitted, wherein
said determining whether said forwarding is permitted is based, at least in
part, on said SGI; and
forwarding said packet via said tunnel, if said forwarding said packet via said
tunnel is permitted.
11. (Previously Presented) The method of claim 10, wherein
said determining whether said forwarding is permitted is based, at least in part, on
a result of said classifying said packet.

12.-13. (Cancelled)

14. (Previously Presented) The method of claim 11, wherein said determining whether said forwarding is permitted comprises:
generating an index, wherein said index comprises said SGI; and
using said index to access an access control list (ACL), wherein said ACL includes information as to whether said packet can be sent via said tunnel.

15. (Original) The method of claim 14, wherein said information comprises:
an SGI field; and
a tunnel identifier field.

16. (Previously Presented) The method of claim 10, wherein said forwarding said packet comprises forwarding said packet from an ingress router to an egress router via said tunnel.

17. (Original) The method of claim 16, further comprising:
receiving said packet at said egress router; and
determining whether said packet can be forwarded by said egress router based on said SGI.

18. (Previously Presented) The method of claim 17, wherein said determining whether said packet can be forwarded by said egress router further comprises:
determining whether said packet can be forwarded by said egress router based, at least in part, on said SGI, a destination of said packet, and an identifier of said tunnel.

19. (Previously Presented) The method of claim 17, wherein said determining whether said packet can be forwarded by said egress router further comprises:
generating an index into an access control list (ACL), wherein

said ACL comprises information regarding whether said packet can be forwarded by said egress router, and
said index includes said identifier of said tunnel; and
accessing said ACL using said index.

20. **(Currently Amended)** A computer system comprising:
a processor;
computer readable storage medium coupled to said processor; and
computer code, encoded in said computer readable storage medium, configured to cause said processor to:
assign a security group identifier (SGI) to a packet, wherein
said SGI is assigned based, at least in part, on a security group of a sender of said packet,
said SGI identifies said security group,
said security group is configured to represent a plurality of senders,
and
said plurality of senders comprises said sender;
generate a classification of said packet by virtue of being configured to classify said packet based, at least in part, on said SGI;
identify a tunnel identifier of said tunnel based on routing of said packet;
determine whether said packet can be sent via a tunnel based, at least in part, on said classification; and
forward said packet via said tunnel, if said forwarding said packet via said tunnel is permitted.

21. (Cancelled)

22. (Previously Presented) The computer system of claim 20, wherein said computer code is further configured to cause said processor to:
determine a routing of said packet, wherein said classification is also based on said routing.

23. (Cancelled)

24. (Previously Presented) The computer system of claim 20, wherein said computer code configured to cause said processor to determine whether said packet can be sent via said tunnel is further configured to cause said processor to:
generate an index, wherein said index comprises said SGI; and
use said index to access an access control list (ACL), wherein said ACL includes information as to whether said packet can be sent via said tunnel.

25. (Original) The computer system of claim 24, wherein said information comprises:
an SGI field; and
a tunnel identifier field.

26. (Previously Presented) The computer system of claim 20, wherein said forwarding said packet comprises forwarding said packet from an ingress router to an egress router via said tunnel.

27. (Original) The computer system of claim 26, wherein said computer code is further configured to cause said processor to:
receive said packet at said egress router; and
determine whether said packet can be forwarded by said egress router based on said SGI.

28. (Previously Presented) The computer system of claim 27, wherein said computer code configured to cause said processor to determine whether said packet can be forwarded by said egress router is further configured to cause said processor to:
determine whether said packet can be forwarded by said egress router based, at least in part, on said SGI, a destination of said packet, and an identifier of said tunnel.

29. (Original) The computer system of claim 27, wherein said computer code configured to cause said processor to determine whether said packet can be forwarded by said egress router is further configured to cause said processor to:

- generate an index into an access control list (ACL), wherein
 - said ACL comprises information regarding whether said packet can be forwarded by said egress router, and
 - said index includes said identifier of said tunnel; and
- access said ACL using said index.

30. **(Currently Amended)** A computer program product, wherein said computer program product comprises a non-transitory computer-readable storage medium, and further comprising:

- a plurality of instructions, comprising
 - a first set of instructions, executable on a computer system, configured to assign a security group identifier (SGI) to a packet, wherein said first set of instructions are further configured to assign said SGI based, at least in part, on a security group of a sender of said packet,
 - said SGI identifies said security group,
 - said security group is configured to represent a plurality of senders,
 - and
 - said plurality of senders comprises said sender,
- a second set of instructions, executable on said computer system, configured to classify said packet based, at least in part, on said SGI,
- a third set of instructions, executable on said computer system, configured to determine a routing of said packet, wherein said determining said routing is based, at least in part, on said SGI,
- and
- said third set of instructions comprises

a first subset of instructions, executable on said computer system, configured to identify a tunnel, **and**
a second subset of instructions, executable on said computer system, configured to identify a tunnel identifier of said tunnel based on said routing of said packet;

a fourth set of instructions, executable on said computer system, configured to determine whether forwarding said packet via said tunnel is permitted, wherein said fourth set of instructions are further configured to use said SGI, and

a fifth set of instructions, executable on said computer system, configured to forward said packet via said tunnel, if said forwarding said packet via said tunnel is permitted; and

said computer-readable storage medium, wherein said instructions are encoded in said computer-readable storage medium.

31. (Previously Presented) The computer program product of claim 30, wherein said second set of instructions is further configured to generate a classification of said packet, and said fourth set of instructions are further configured to use said classification.

32.-33. (Cancelled)

34. (Previously Presented) The computer program product of claim 31, wherein said fourth set of instructions comprises:
a first subset of instructions, executable on said computer system, configured to generate an index, wherein said index comprises said SGI; and
a second subset of instructions, executable on said computer system, configured to use said index to access an access control list (ACL), wherein said ACL includes information as to whether said packet can be sent via a tunnel.

35. (Original) The computer program product of claim 34, wherein said information comprises:

- an SGI field; and
- a tunnel identifier field.

36. (Previously Presented) The computer program product of claim 30, wherein

- said fifth set of instructions are further configured to forward said packet from an ingress router to an egress router via said tunnel.

37. (Previously Presented) The computer program product of claim 36, further comprising:

- a sixth set of instructions, executable on said computer system, configured to receive said packet at said egress router; and
- a seventh set of instructions, executable on said computer system, configured to determine whether said packet can be forwarded by said egress router based on said SGI.

38. (Previously Presented) The computer program product of claim 37, wherein said seventh set of instructions comprises:

- a first subset of instructions, executable on said computer system, configured to determine whether said packet can be forwarded by said egress router based, at least in part, on said SGI, a destination of said packet, and an identifier of said tunnel.

39. (Previously Presented) The computer program product of claim 37, wherein said seventh set of instructions comprises:

- a first subset of instructions, executable on said computer system, configured to generate an index into an access control list (ACL), wherein said ACL comprises information regarding whether said packet can be forwarded by said egress router, and said index includes said identifier of said tunnel; and

a second subset of instructions, executable on said computer system, configured to access said ACL using said index.

40. **(Currently Amended)** An apparatus comprising:

a processor;

a memory, coupled to the processor;

means for assigning a security group identifier (SGI) to a packet, wherein
said means for assigning said SGI is configured to assign said SGI based,
at least in part, on a security group of a sender of said packet,
said SGI identifies said security group,
said security group is configured to represent a plurality of senders, and
said plurality of senders comprises said sender;

means for classifying said packet based, at least in part, on said SGI, wherein
said means for classifying is coupled to said means for assigning, and
said means for classifying comprises the memory;

means for determining a routing of said packet, wherein
said means for determining said routing comprises the processor,
said means for determining said routing is configured to determine said
routing based, at least in part, on said SGI, and
said determining said routing comprises
identifying a tunnel;

**means for identifying a tunnel identifier of said tunnel based on said routing
of said packet;**

means for determining whether forwarding said packet via said tunnel is
permitted, wherein
said means for determining whether said forwarding is permitted is
configured to make a determination as to whether said forwarding
is permitted based, at least in part, on said SGI; and
means for forwarding said packet via said tunnel, if said forwarding said packet
via said tunnel is permitted, wherein
said means for forwarding is coupled to said means for determining.

41. (Previously Presented) The apparatus of claim 40, wherein said means for determining whether said forwarding is permitted is configured to make a determination as to whether said formatting is permitted based, at least in part, on a result generated by said means for classifying said packet.
42. (Cancelled)
43. (Cancelled)
44. (Previously Presented) The apparatus of claim 41, wherein said means for determining whether said forwarding is permitted comprises:
means for generating an index, wherein said index comprises said SGI; and
means for using said index to access an access control list (ACL), wherein said ACL includes information as to whether said packet can be sent via said tunnel.
45. (Original) The apparatus of claim 44, wherein said information comprises:
an SGI field; and
a tunnel identifier field.
46. (Previously Presented) The apparatus of claim 40, wherein said means for forwarding said packet is configured to forward said packet from an ingress router to an egress router via said tunnel.
47. (Original) The apparatus of claim 46, further comprising:
means for receiving said packet at said egress router; and
means for determining whether said packet can be forwarded by said egress router based on said SGI.

48. (Previously Presented) The apparatus of claim 47, wherein said means for determining whether said packet can be forwarded by said egress router further comprises:

means for determining whether said packet can be forwarded by said egress router based, at least in part, on said SGI, a destination of said packet, and an identifier of said tunnel.

49. (Previously Presented) The apparatus of claim 47, wherein said means for determining whether said packet can be forwarded by said egress router further comprises:

means for generating an index into an access control list (ACL), wherein said ACL comprises information regarding whether said packet can be forwarded by said egress router, and said index includes said identifier of said tunnel; and means for accessing said ACL using said index.